UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 14-118
	)	
WANG DONG,	)	
a/k/a "Jack Wang,"	)	
a/k/a "UglyGorilla,"	)	
SUN KAILIANG,	)	18 U.S.C. § 1030(a)(2)(C),
a/k/a "Sun Kai Liang,"	)	1030(a)(5)(A), 1030(b)
a/k/a "Jack Sun,"	)	18 U.S.C. § 1028A,
WEN XINYU,	)	18 U.S.C. § 1831(a)(2),
a/k/a "Wen Xin Yu,"	)	(a)(4), and
a/k/a "WinXYHappy,"	)	18 U.S.C. § 1832(a)(2),
a/k/a "Win_XY,"	)	(a)(4)
a/k/a "Lao Wen,"	)	
HUANG ZHENYU,	)	
a/k/a "Huang Zhen Yu,"	)	**UNDER SEAL**
a/k/a "hzy_lhx," and	)	
GU CHUNHUI,	)	
a/k/a "Gu Chun Hui,"	)	
a/k/a "KandyGoo,"	)	

FILED

MAY - 1 2014

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

INDICTMENT

COUNT ONE
(Conspiracy to Commit Computer Fraud and Abuse)

The Grand Jury Charges:

INTRODUCTION

1. From at least in or about 2006 up to and including at least in or about April 2014, members of the People's Liberation Army ("PLA"), the military of the People's Republic of China ("China"), conspired together and with each other to hack into the computers of commercial entities located in the Western District of Pennsylvania and elsewhere in the United States, to maintain unauthorized access to those computers, and to steal

information from those entities that would be useful to their competitors in China, including state-owned enterprises ("SOEs").

2. In some cases, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. For example, as described in more detail below, an Oregon producer of solar panel technology was rapidly losing its market share to Chinese competitors that were systematically pricing exports well below production costs; at or around the same time, members of the conspiracy stole cost and pricing information from the Oregon producer. And while a Pennsylvania nuclear power plant manufacturer was negotiating with a Chinese company over the construction and operation of four power plants in China, the conspirators stole, among other things, proprietary and confidential technical and design specifications for pipes, pipe supports, and pipe routing for those nuclear power plants that would enable any competitor looking to build a similar plant to save on research and development costs in the development of such designs.

3. In the case of both of those American victims and others, the conspirators also stole sensitive, internal communications that would provide a competitor, or adversary in

litigation, with insight into the strategy and vulnerabilities of the American entity.

4. Meanwhile, during the period relevant to this Indictment, Chinese firms hired the same PLA Unit where the defendants worked to provide information technology services. For example, one SOE involved in trade litigation against some of the American victims mentioned herein hired the Unit, and one of the co-conspirators charged herein, to build a "secret" database to hold corporate "intelligence."

THE DEFENDANTS

5. At various times relevant to this Indictment, Defendants WANG DONG, a/k/a "Jack Wang," a/k/a "UglyGorilla" (hereinafter "Defendant WANG"); SUN KAILIANG, a/k/a "Sun Kai Liang," a/k/a "Jack Sun" (hereinafter "Defendant SUN"); WEN XINYU, a/k/a "Wen Xin Yu," a/k/a "WinXYHappy," a/k/a "Win_XY," a/k/a "Lao Wen" (hereinafter "Defendant WEN"); HUANG ZHENYU, a/k/a "Huang Zhen Yu," a/k/a "hzy_lhx," (hereinafter "Defendant HUANG"); and GU CHUNHUI, a/k/a "Gu Chun Hui," a/k/a "KandyGoo" (hereinafter "Defendant GU"), whose photographs are attached as Exhibits A through E, respectively, worked together and with others known and unknown to the Grand Jury for the PLA's General Staff, Third Department ("3PLA"), a signals intelligence component of the PLA, in a Unit known by the Military Unit Code

Designator 61398 ("Unit 61398"), and in the vicinity of 208 Datong Road, Pudong District, Shanghai, China.

6. The co-conspirators' hacking activities are described in more detail below but are summarized here as follows:

a. In or about 2007, Westinghouse Electric Company ("Westinghouse"), which is headquartered in the Western District of Pennsylvania, reached an agreement with a Chinese state-owned nuclear power company ("SOE-1") to construct and operate four nuclear power plants in China. Negotiations regarding the details of that transaction, such as limitations on which technology would be provided to SOE-1 and under what conditions, continued up to and including 2013. In or about 2010 and 2011, while negotiations were ongoing, Defendant SUN stole from Westinghouse's computers, among other things, proprietary and confidential technical and design specifications for pipes, pipe supports, and pipe routing within the nuclear power plants that Westinghouse was contracted to build, as well as internal Westinghouse communications concerning the company's strategy for doing business with SOE-1 in China and the potential that SOE-1 may eventually become a competitor.

b. In or about May and July 2012, Defendant WEN hacked into the computers of U.S. subsidiaries of SolarWorld AG, a German solar products manufacturing company, including a production facility located in Hillsboro, Oregon, and a sales

facility located in Camarillo, California (collectively, "SolarWorld"). From in or about May 2012 up to and including at least in or about September 2012, Defendant WEN and at least one unidentified co-conspirator stole thousands of e-mails and related attachments that provided detailed information about SolarWorld's financial position, production capabilities, cost structure, and business strategy. Meanwhile, contemporaneous with that hacking, SolarWorld was an active litigant in trade cases against Chinese solar manufacturers, several of which reported in filings with the U.S. Securities and Exchange Commission ("SEC") that their sales revenues had increased each year from 2009 through 2011. In or about May 2012, the Department of Commerce imposed significant duties on Chinese imports of solar products, based on its finding that those manufacturers had received unfair subsidies from China and had "dumped" large volumes of solar products into U.S. markets at prices below fair value, severely undercutting competitors like SolarWorld and, in some cases, helping to drive the most vulnerable American solar products manufacturers out of business. Several Chinese solar manufacturers subsequently reported in SEC filings that, in 2012, their sales revenues had decreased from 2011, and their net income and profit margins had dropped to five-year lows.

c. Between in or about 2009 and in or about 2012, United States Steel Corporation ("U.S. Steel"), which is headquartered in the Western District of Pennsylvania, litigated a number of trade cases against the Chinese steel industry, including specifically one large, Chinese state-owned steel company ("SOE-2"). About two weeks before the anticipated decision in one of those disputes in 2010, Defendant SUN targeted one of the employees working in the relevant division of U.S. Steel with an e-mail message, known as a "spearphishing" message, that was designed to trick the employee who received it into allowing SUN access to the employee's computer. At or about that time, Defendant WANG stole hostnames and descriptions for more than 1,700 servers, including servers that controlled physical access to the company's facilities and mobile device access to the company's networks.

d. Allegheny Technologies Incorporated ("ATI"), a specialty metals manufacturer headquartered in the Western District of Pennsylvania, has since in or about 1995 been a partner in a joint venture with SOE-2 and was, between 2009 and 2012, also an adversary of SOE-2 in litigation before the World Trade Organization ("WTO"). In April 2012, the day after a board meeting for the joint venture in Shanghai, China, Defendant WEN stole network credentials for virtually every

employee at the company, which would have allowed wide-ranging and persistent access to ATI's computers.

e. The United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union ("USW"), headquartered in the Western District of Pennsylvania, has long been a vocal opponent of Chinese trade practices. In 2012, on or about the day that the USW's President issued a "call to action" against Chinese policies, Defendant WEN stole e-mail messages containing strategic discussions from senior union employees. And two days after the union publicly urged Congress to pass legislation that would have imposed duties on Chinese imports, Defendant WEN stole more e-mail messages containing internal, strategic discussions.

f. In or about 2008, Alcoa Incorporated ("Alcoa"), an aluminum manufacturer whose principal office is located in the Western District of Pennsylvania, announced a partnership with a Chinese state-owned aluminum company to acquire a stake in another foreign mining company. Approximately three weeks later, Defendant SUN targeted senior Alcoa managers with spearphishing messages designed to trick the recipients into providing SUN with access to the company's computers.

7. As described above, Defendants WANG, SUN, and WEN, among others known and unknown to the Grand Jury, hacked or

attempted to hack into at least the U.S. companies described above.

8. Contemporaneously, beginning at least in or about 2006 and continuing until at least in or about 2012, Defendant HUANG was a computer programmer within the same military Unit. He facilitated hacking activities by registering and managing domain accounts that his co-conspirators, including at least Defendants WANG, SUN, and WEN, used to commit those crimes. Meanwhile, beginning at least in or about 2006 and continuing until at least in or about 2009, Unit 61398 assigned Defendant HUANG to perform programming work for SOE-2, including the creation of a "secret" database for SOE-2 designed to hold corporate "intelligence" about the iron and steel industries, including information about American companies.

9. Like Defendant HUANG, beginning at least in or about 2006 and continuing until at least in or about 2010, Defendant GU managed domain accounts used to facilitate hacking activities against American companies. Defendant GU also tested spearphishing messages in furtherance of the conspiracy.

MANNER AND MEANS OF THE CONSPIRACY

10. The members of the conspiracy, who are both known and unknown to the Grand Jury, used the following manner and means to accomplish their objectives, which included gaining

unauthorized access to computers and using that access to steal information.

11. As described above, the co-conspirators used e-mail messages known as "spearphishing" messages to trick unwitting recipients into giving the co-conspirators access to their computers. Spearphishing messages were typically designed to resemble e-mails from trustworthy senders, like colleagues, and encouraged the recipients to open attached files or click on hyperlinks in the messages. However, the attached or linked files, once opened, installed "malware" --- malicious code --- that provided unauthorized access to the recipient's computer (known as a "backdoor"), thereby allowing the co-conspirators to bypass normal authentication procedures in the future.

12. After creating a backdoor, the malware typically attempted to contact other computers controlled by the co-conspirators by sending them a short message known as a "beacon." These beacons typically (1) notified the co-conspirators of the successful penetration of a victim's computer; (2) provided some information about the victim's computer useful for future intrusion activity; and (3) solicited additional instructions from the co-conspirators.

13. During the conspiracy, the co-conspirators controlled compromised computers in the United States besides those belonging to the six entities named above. The co-conspirators

generally used those computers, known as "hop points," to access other victims' computers, and in so doing, the co-conspirators attempted to mask the true identity and location of the computers in China from which they were actually conducting their hacking activity. Among other things, the co-conspirators used hop points to research victims, send spearphishing e-mails, store and distribute additional malware, manage malware, and transfer exfiltrated data. Some hop points were used as command-and-control servers, which received communications from, and returned instructions to, malware on other compromised computers.

14. The co-conspirators commonly used domain names to hide malicious communications to and from hop points and other victim computers. "Domain names" are labels used to indicate ownership or control of a resource on the Internet, and they are governed by the rules and procedures of the Domain Name System ("DNS"). Domain names resolve back to specific Internet Protocol (or simply "IP") addresses, which are unique, numeric addresses assigned to computers to route traffic on the Internet.

15. The function of the DNS is to translate an alphanumeric domain name into an IP address of the computer hosting that domain; using the DNS is analogous to using a phone book to look up the phone number of a particular person. Typically, an Internet user attempts to navigate to a website

using its domain name, but computers navigate to a website using an IP address. When a computer user types the domain "websitename.com" into a web browser, for example, the user's computer contacts a DNS server, which then translates the domain name into an IP address, like "58.247.27.223," and sends that IP address back to the user's computer. The user's computer can then immediately communicate directly with websitename.com, because it has identified the corresponding IP address. Dynamic DNS providers enable owners or operators of domain names to change the IP addresses to which the domain names resolve, usually by logging into domain accounts at the providers over the Internet and configuring the settings for the domain names to include the destination IP addresses.

16. The co-conspirators, either directly or through intermediaries, purchased, leased, or otherwise registered domain names from domain registrars, obtained accounts at dynamic DNS providers, and assigned the domain names to those domain accounts (if the domain names were not already assigned to the desired DNS providers as part of the original purchase, lease, or registration). Using those domain accounts, the co-conspirators managed the resolutions of those domain names (that is, the assignments of those domain names to particular IP addresses on the Internet, to which lookup requests for those domain names would be directed). Often, those domain names were

designed to mimic the domain names of legitimate websites, but with slight differences in spelling, such as "finaceanalysis.com," "gmailboxes.com," and "busketball.com." The co-conspirators then used the domain names with their malware. After the malware was installed on victim computers, the domain names served as the destination points for the malware to contact, or beacon, for further instructions. The table below lists some of the other malicious domains used by the conspiracy during the period relevant to this Indictment:

Malicious Domain Names
arrowservice.net
bigish.net
businessconsults.net
businessformars.com
marsbrother.com
purpledaily.com
newsonet.net
comrepair.com
oplaymagzine.com
hugesoft.org

17. The co-conspirators used the domain accounts at dynamic DNS providers to assign their domain names to the IP addresses of different computers depending on their needs at the time. For example, when the co-conspirators wished to proceed with particular intrusions, they used the applicable accounts at dynamic DNS providers to turn malicious domains associated with their malware "on," that is, to assign the domains to the IP addresses of computers under their control, like hop points. Then, between intrusions, the co-conspirators used the domain

accounts to reassign the malicious domain names to non-routable or innocuous IP addresses (e.g., IP addresses for popular webmail services, like Gmail or Yahoo), which would obscure any beacons their malware sent during that period. At one dynamic DNS provider, for example, domains were typically turned "on" at the beginning of business hours in Shanghai, Monday through Friday, and turned "off" (reassigned to non-routable or innocuous IP addresses) at lunchtime and the close of business, and left off over the weekend, as the charts attached as Exhibit F to this Indictment show.

18. After obtaining a foothold in a victim's computers, the co-conspirators performed a variety of functions designed to identify, collect, package, and exfiltrate targeted data from the victim's computers to other computers under the co-conspirators' control.

THE CONSPIRACY'S INTRUSIONS AT SIX VICTIMS

Westinghouse

19. Westinghouse is one of the world's leading civilian nuclear power developers, providing fuel, services, and plant design to customers in the commercial nuclear industry worldwide. The company's designs are the basis for approximately half of the world's currently operating nuclear power plants. Westinghouse's AP1000 Nuclear Power Plant is a particularly well-known power plant design, with unique safety

features, which took Westinghouse significant resources to develop over a 15-year period.

20. After two years of negotiations, on July 24, 2007, Westinghouse and SOE-1, a Chinese state-owned enterprise in the nuclear power industry, signed contracts for the construction and operation of four AP1000 power plants in China, subject to further negotiations on certain unresolved issues. Those contracts provided for the transfer of some technology to SOE-1, but they limited what SOE-1 was permitted to do with it. For example, SOE-1 was not authorized to send materials and components outside China, to use them in reactor plants that competed with Westinghouse's products outside China, or to use them for military purposes. Further, the technology transfer contracts limited SOE-1's ability to provide such technologies to entities other than those listed in the contracts without notifying and receiving approval from Westinghouse. Negotiations regarding the other details, including additional technology transfer issues, continued for years thereafter, up to and including 2013.

21. During the conspiracy, while Westinghouse was building the AP1000 plants and negotiating other terms with SOE-1, hackers repeatedly targeted Westinghouse's computers, including computers in the Western District of Pennsylvania. For example, on or about May 6, 2010, Defendant SUN gained unauthorized

access to Westinghouse's computers and stole proprietary and confidential technical and design specifications related to pipes, pipe supports, and pipe routing within the AP1000 plant buildings. Among other things, such specifications would enable a competitor to build a plant similar to the AP1000 without incurring significant research and development costs associated with designing similar pipes, pipe supports, and pipe routing systems. During the same intrusion, Defendant SUN also stole Westinghouse network credentials that would facilitate additional, unauthorized access.

22. In addition to constructing the AP1000 plants and negotiating contractual details relating to those plants, in late 2010, Westinghouse began to explore other business ventures with SOE-1. For example, in or about September 2010, Westinghouse and SOE-1 began negotiating over the construction of additional power plants in China. Westinghouse sought to conclude these negotiations before the arrival of an SOE-1 official in Washington, D.C., as part of a January 2011 Chinese state visit, so that the agreement could be signed during the visit. Meanwhile, Westinghouse management internally discussed what approach to take during upcoming negotiations and in future partnerships with SOE-1, as well as the potential that SOE-1 may eventually become a competitor.

23. While these business initiatives and discussions were underway, beginning at least in or about December 2010 and continuing until at least in or about January 2011, Defendant SUN repeatedly targeted Westinghouse's computers. For example, on or about December 30, 2010, January 3, 2011, and January 5, 2011, Defendant SUN gained unauthorized access to Westinghouse's computers and stole sensitive, non-public, and deliberative e-mails belonging to senior decision-makers responsible for Westinghouse's business relationship with SOE-1, including Westinghouse's Chief Executive Officer. Some stolen e-mails described the status of the four AP1000 plants' construction. Many other stolen e-mails, however, concerned Westinghouse's confidential business strategies relating to SOE-1, including Westinghouse's (a) strategies for reaching an agreement with SOE-1 on future nuclear power plant construction in China; and (b) discussions regarding cooperation and potential future competition with SOE-1 in the development of nuclear power plants elsewhere around the world.

24. In total, between in or about 2010 and in or about 2012, members of the conspiracy stole at least 1.4 gigabytes of data, the equivalent of roughly 700,000 pages of e-mail messages and attachments, from Westinghouse's computers.

SolarWorld

25. At times relevant to this Indictment, SolarWorld had significant business interests relating to China, including as a direct competitor with various Chinese solar products manufacturers. Beginning at least in or about October 2011 and continuing until in or about September 2012, SolarWorld was particularly active in trade litigation involving Chinese manufacturers: it was the lead petitioner in a case before the U.S. Department of Commerce and U.S. International Trade Commission. That litigation ultimately resulted in a finding that Chinese solar manufacturers had received unfair subsidies from China and had "dumped" large volumes of solar products into U.S. markets at prices below fair value. As a result, the Department of Commerce imposed significant countervailing and antidumping duties on Chinese imports of solar products.

26. On or about May 3, 2012, following one preliminary determination by the Department of Commerce and about two weeks before a second determination was scheduled, Defendant WEN hacked into SolarWorld's computers and stole e-mails and files belonging to three senior executives. Then, from on or about May 9, 2012 up to and including on or about September 26, 2012, Defendant WEN and at least one other, unidentified co-conspirator conducted at least twelve more intrusions into and exfiltrations from SolarWorld's computers. Through those

intrusions, they stole thousands of e-mail messages and other files from at least seven identified SolarWorld employees who, based on their positions, would be expected to have comprehensive and highly detailed information about SolarWorld's financial position, production capabilities, cost structure, business strategy, or trade litigation strategy.

27. Collectively, the data stolen from SolarWorld would have enabled a Chinese competitor to target SolarWorld's business operations aggressively from a variety of angles. For example, the stolen data included: (1) cash-flow spreadsheets maintained by the Chief Financial Officer that would enable a Chinese competitor to identify the length of time that SolarWorld might survive a financial or market shock; (2) detailed manufacturing metrics, technological innovations, and production line information that would enable a Chinese competitor to mimic SolarWorld's proprietary production capabilities without the need to invest time or money in research and development; (3) specific production costs for all manufacturing inputs that would enable a Chinese competitor to undermine SolarWorld financially through targeted and sustained underpricing of solar products; and (4) privileged attorney-client communications related to SolarWorld's ongoing trade litigation with China, including confidential Question-and-

Answer documents submitted to the Department of Commerce that were not discoverable by the Chinese respondents.

U.S. Steel

28. U.S. Steel is the largest steel company in the United States. During the period relevant to this Indictment, U.S. Steel had significant business interests relating to China, including as a competitor of several Chinese steel manufacturers like SOE-2. For example, beginning at least in or about 2009 and continuing until at least in or about 2012, U.S. Steel participated in several international trade disputes with Chinese steel manufacturers, including SOE-2. These disputes involved allegations that China subsidized the Chinese steel industry and that the Chinese steel industry "dumped" steel into U.S. markets at below-market prices.

29. In or about 2010, U.S. Steel was particularly active in that litigation. That year, U.S. Steel was one of several lead petitioners in protracted litigations before the U.S. Department of Commerce and U.S. International Trade Commission involving imports of (a) oil country tubular goods ("OCTG"), which are steel piping used by oil and gas companies; and (b) seamless standard line pipes ("SSLP"), which are steel pipes specifically constructed without a welded seam down the length of the pipes. In both cases, the Department of Commerce found that the respondents --- various Chinese steel manufacturers

including SOE-2 --- received unfair subsidies from China and "dumped" billions of dollars' worth of steel into U.S. markets at prices below fair value. As a result, the Department of Commerce imposed significant countervailing and antidumping duties worth millions of dollars on Chinese imports of OCTG and SSLP. Thereafter, the amount of OCTG and SSLP steel imported by Chinese manufacturers fell dramatically.

30. In or about February 2010, while U.S. Steel was participating in at least the two international trade disputes described above, Defendants SUN and WANG hacked into U.S. Steel's computers.

a. On or about February 8, 2010, approximately two weeks before the U.S. Department of Commerce was scheduled to release its preliminary determination in the SSLP trade dispute, Defendant SUN sent a spearphishing e-mail purporting to be from U.S. Steel's Chief Executive Officer to approximately 20 U.S. Steel employees affiliated with the U.S. Steel division responsible for OCTG and SSLP. The e-mail contained a link to malware, which some of the recipients clicked on, installing malware on computers located in the Western District of Pennsylvania and providing Defendant SUN and his co-conspirators with backdoor access to U.S. Steel's computers.

b. On or about February 23, 2010, Defendant SUN sent spearphishing e-mails purporting to be from two U.S. Steel e-

mail accounts to approximately eight U.S. Steel employees, including U.S. Steel's Chief Executive Officer. The e-mails had the subject line "US Steel Industry Outlook" and contained a link to malware that, once clicked, would surreptitiously install malware on the recipients' computers, allowing the co-conspirators backdoor access to the company's computers. Further, beginning on or about February 24, 2010 and continuing until on or about March 2, 2010, an unidentified co-conspirator sent approximately 49 spearphishing e-mails to U.S. Steel employees with the same subject, "US Steel Industry Outlook."

c. On or about February 26, 2010, Defendant WANG gained unauthorized access to at least one U.S. Steel computer located in the Western District of Pennsylvania. Defendant WANG used that unauthorized access to steal hostnames and descriptions for more than 1,700 U.S. Steel computers, including servers used for emergency response, network monitoring, network security, applications for U.S. Steel employees' mobile devices, and physical access to U.S. Steel's facilities in the Western District of Pennsylvania. WANG then took steps to identify and exploit vulnerable servers on that list.

ATI

31. ATI is a large specialty metals company. It operates primarily in three business segments: high performance metals

(e.g., nickel and cobalt), flat-rolled products (e.g., stainless steel), and engineered products (e.g., tungsten).

32. At times relevant to this Indictment, ATI had significant business interests relating to China, including as a partner with and competitor of various Chinese producers of flat-rolled products. For example, since approximately 1995, ATI, through a wholly owned subsidiary, has partnered in a joint venture with SOE-2 for the manufacture of precision rolled stainless steel strips, which are, among other things, used in the automotive, medical equipment, and semiconductor industries. The board of directors of this joint venture met periodically including, for example, on or about April 12, 2012, in Shanghai, China. That same ATI subsidiary competed with SOE-2 in the production of grain oriented flat-rolled electrical steel ("GOES"), which is used in power distribution and power generation transformers. In addition, beginning at least in or about June 2009 and continuing until at least in or about June 2012, ATI participated in an international trade dispute against SOE-2 regarding ATI's importation of GOES into China, which the WTO ultimately resolved in ATI's favor.

33. On or about April 13, 2012, the day after the joint venture board meeting, Defendant WEN gained unauthorized access into ATI computers located in the Western District of Pennsylvania. Defendant WEN then stole the usernames and

passwords for at least 7,000 ATI employees. These network credentials would have facilitated additional unauthorized access to ATI's computers by Defendant WEN and his co-conspirators, allowing them to monitor activity on those systems and to steal ATI's information in the future.

34. Thereafter, on at least three occasions in or about May 2012, several of the same compromised ATI computers beaconed to the same hop point used to steal those network credentials, reflecting persistent access by the hackers.

<u>USW</u>

35. USW has approximately one million active and retired members nationwide from a variety of industries including metals, energy, and rubber and plastics. One of USW's core missions is to oppose Chinese trade practices that it perceives as unfair. USW's trade strategy includes representing its members in international trade disputes, media campaigns, and lobbying. On at least four occasions between in or about 2010 and 2012 --- while USW was particularly vocal about China's trade practices --- Defendant WEN and an unidentified co-conspirator gained unauthorized access to USW's computers and stole e-mail messages and attachments from the accounts of six to eight USW employees who would be expected to have sensitive, non-public, and deliberative information about USW's trade

strategy concerning China. Each theft targeted messages from a narrow window of time before the intrusion.

36. For example, in or about late January 2012, USW was involved in public disputes over Chinese trade practices in at least two industries, raw materials and auto parts. First, on or about January 30, 2012, the Appellate Body of the WTO issued a report concluding that Chinese trade practices relating to the export of various industrial raw materials were inconsistent with China's obligations as a member of the WTO. In response and on the same day, USW issued a press release stating that the decision was "a huge victory for American workers." And the next day, on or about January 31, 2012, USW issued a statement from its International President, calling on the U.S. Government to take action to protect the U.S. auto parts sector from "China's predatory, protectionist and illegal trade practices." USW also released a report on Chinese trade practices in the auto parts industry.

37. That same day, on or about January 31, 2012, Defendant WEN gained unauthorized access to USW's computers, and stole e-mails dated between in or about January 24 and January 31, 2012 that were located in certain folders of the accounts of six senior USW employees, including USW's International President, most of whom were personally and publicly involved in either the raw materials or auto parts disputes. The stolen e-mails

included sensitive, non-public, and deliberative information about USW's strategy including, for example, USW's preparations for the January 31, 2012 news conference where it issued its "call to action" against Chinese trade practices in the auto parts sector; discussion of the merits of the January 31, 2012 WTO report on raw materials; and drafts of press releases announcing that report.

38. Then, on or about March 5, 2012, the International President of USW issued an open letter urging Congress to pass a bill that would grant the U.S. Department of Commerce authority to impose countervailing duties on Chinese exports, stating "[i]t would be a travesty for Congress to stand idle while a country like China . . . can provide lavish subsidies for exports without the United States being able to defend American workers and producers by offsetting the harm." Approximately two days later, on or about March 7, 2012, Defendant WEN again gained unauthorized access to USW's computers and stole e-mails received between March 1 and March 7, 2012 from the inboxes of six senior USW employees, including USW's International President. Those e-mails included sensitive, non-public, and deliberative information about USW's trade strategy, such as internal discussions of how USW would change its strategy in pending international trade disputes if the bill were enacted, and the union's decision not to seek an extension of certain

tariffs against Chinese companies, which USW had not yet announced.

39. Thereafter, until at least in or about January 2013, USW computers continued to beacon to malicious domains used by the conspiracy on a near daily basis, reflecting persistent access by the co-conspirators to USW's computers.

Alcoa

40. Alcoa is the largest aluminum company in the United States. At times relevant to this Indictment, Alcoa had significant business interests relating to China. For example, in or about 2001, Alcoa entered into an agreement with a Chinese SOE in the aluminum industry ("SOE-3") to purchase shares in a Chinese aluminum company that SOE-3 partially owned. Alcoa sold those shares on or about September 12, 2007. Then, on or about February 1, 2008, Alcoa announced a partnership with SOE-3 to acquire a substantial stake in a foreign mining company.

41. Spearphishing activity targeted Alcoa including near in time to significant events in its business relationship with SOE-3. For example, on or about February 20, 2008, about three weeks after Alcoa announced the partnership with SOE-3, Defendant SUN targeted Alcoa with a spearphishing campaign. Specifically, Defendant SUN sent e-mails to approximately 19 senior Alcoa employees, at least some of whom were located in the Western District of Pennsylvania, using an account designed

to impersonate a member of Alcoa's Board of Directors. In all but one of the e-mails, Defendant SUN attached a file disguised as an agenda for Alcoa's annual shareholders meeting, which, once opened, would install malware on the recipients' computers.

42. Thereafter, in or about June 2008, unidentified individuals stole at least 2,907 e-mail messages along with approximately 863 attachments from Alcoa's computers, including internal messages among Alcoa senior managers discussing the foregoing acquisition.

STATUTORY ALLEGATIONS

43. Beginning at least in or about 2006 and continuing until at least in or about April 2014, the exact dates being unknown to the Grand Jury, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
a/k/a "Jack Wang,"
a/k/a "UglyGorilla,"
SUN KAILIANG,
a/k/a "Sun Kai Liang,"
a/k/a "Jack Sun,"
WEN XINYU,
a/k/a "Wen Xin Yu,"
a/k/a "WinXYHappy,"
a/k/a "Win_XY,"
a/k/a "Lao_Wen,"
HUANG ZHENYU,
a/k/a "Huang Zhen Yu,"
a/k/a "hzy_lhx," and
GU CHUNHUI,
a/k/a "Gu Chun Hui,"
a/k/a "KandyGoo,"

did knowingly and intentionally combine, conspire, confederate, and agree together, with each other and with others known and unknown to the Grand Jury, to commit offenses against the United States, namely:

a. to access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, for the purpose of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the laws of the Commonwealth of Pennsylvania, namely, the common law tort of Invasion of Privacy, and where the value of the information did, and would if completed, exceed $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B); and

b. to cause the transmission of a program, information, code, and command, and as a result of such conduct, to cause damage without authorization to a protected computer, and where the offense did cause and would, if completed, have caused, loss aggregating $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least 10 protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

OVERT ACTS

44. In furtherance of the conspiracy and to achieve the objects thereof, the conspirators committed the following overt acts, among others, in the Western District of Pennsylvania and elsewhere:

a. On or about April 18, 2006, Defendant SUN created e-mail account c********8@yahoo.com.

b. On or about July 17, 2006, Defendant SUN created domain account j*****r at a domain provider in the United States.

c. On or about December 12, 2006, Defendant WEN sent Defendant WANG two executable files containing tools that would be useful for intrusions.

d. On or about July 12, 2007, Defendant GU designed and tested a spearphishing message.

e. On or about February 20, 2008, Defendant SUN created an e-mail account using the misspelled name of a person with the initials C.G., who was then a member of Alcoa's Board of Directors (the "C.G. Spearphishing Account").

f. On or about February 20, 2008, Defendant SUN, using the C.G. Spearphishing Account, transmitted e-mail messages with a file named "agenda.zip," which contained malware, to approximately 19 Alcoa employees.

g. On or about October 26, 2008, Defendant GU designed and tested a spearphishing message.

h. On or about February 8, 2010, Defendant SUN sent a spearphishing e-mail purporting to be from U.S. Steel's Chief Executive Officer to approximately 20 U.S. Steel employees.

i. On or about February 23, 2010, Defendant SUN sent spearphishing e-mails purporting to be from two U.S. Steel e-mail accounts to approximately eight U.S. Steel employees.

j. On or about February 26, 2010, Defendant WANG accessed without authorization at least one U.S. Steel computer located in the Western District of Pennsylvania.

k. On or about February 26, 2010, Defendant WANG stole server names and descriptions from a U.S. Steel computer located in the Western District of Pennsylvania.

l. On or about February 26, 2010, Defendant WANG transmitted at least one file that he stole from a U.S. Steel computer to a computer located in China.

m. On or about February 26, 2010, Defendant WANG transmitted a file named "ccapp.exe" to a U.S. Steel computer.

n. On or about May 6, 2010, Defendant SUN accessed without authorization a Westinghouse computer located in the Western District of Pennsylvania with hostname L******0.

o. On or about May 6, 2010, Defendant SUN transmitted a file named "ccapp.exe" to a Westinghouse computer

located in the Western District of Pennsylvania with hostname L******0.

p. On or about May 6, 2010, Defendant SUN transmitted a file named "ccapp.exe" to a Westinghouse computer with the hostname W*****9.

q. On or about May 6, 2010, Defendant SUN stole at least one file from a Westinghouse computer with hostname W*****9.

r. On or about August 24, 2010, Defendant WEN sent a test spearphishing e-mail to Defendant SUN.

s. On or about December 30, 2010, Defendant SUN accessed the malicious domain account "purpledaily.com" and changed the IP address of sub-domain "klwest.purpledaily.com" to a hop point located in Kansas.

t. On or about December 30, 2010, Defendant SUN accessed without authorization a Westinghouse computer with hostname L******9.

u. On or about December 30, 2010, Defendant SUN transmitted a file named "ccapp.exe" to a Westinghouse computer with hostname L******9.

v. On or about December 30, 2010, Defendant SUN transmitted at least two files named "wiam.exe" and "ccapp.exe" to a Westinghouse computer located in the Western District of Pennsylvania with hostname T********4.

w. On or about December 30, 2010, Defendant SUN stole e-mails from the accounts of six Westinghouse employees.

x. On or about January 3, 2011, Defendant SUN accessed without authorization a Westinghouse computer with hostname W*****9.

y. On or about January 3, 2011, Defendant SUN transmitted a file named "ccapp.exe" to a Westinghouse computer with hostname W*****9.

z. On or about January 3, 2011, Defendant SUN transmitted a file named "ccapp.exe" to a Westinghouse computer located in the Western District of Pennsylvania with hostname T********9.

aa. On or about January 3, 2011, Defendant SUN stole e-mails from the accounts of six Westinghouse employees.

bb. On or about January 5, 2011, Defendant SUN accessed the malicious domain account "bigish.net" and changed the IP address assigned to two bigish.net sub-domains, including "finekl.bigish.net," to a hop point located in Kansas.

cc. On or about January 5, 2011, Defendant SUN accessed without authorization a Westinghouse computer located in the Western District of Pennsylvania with hostname L******4.

dd. On or about January 5, 2011, Defendant SUN transmitted files named "wiam.exe" and "ccapp.exe" to a

Westinghouse computer located in the Western District of Pennsylvania with hostname L******4.

ee. On or about January 5, 2011, Defendant SUN transmitted files named "wiam.exe" and "ccapp.exe" to a Westinghouse computer with hostname L******5.

ff. On or about January 5, 2011, Defendant SUN stole e-mails from the accounts of six Westinghouse employees.

gg. On or about January 31, 2012, Defendant WEN accessed without authorization a USW computer located in the Western District of Pennsylvania with hostname J*************6.

hh. On or about January 31, 2012, Defendant WEN transmitted a file named "ccapp.exe" to a USW computer located in the Western District of Pennsylvania with hostname J*************6.

ii. On or about January 31, 2012, Defendant WEN stole hundreds of e-mails from the accounts of six USW employees.

jj. On or about March 7, 2012, Defendant WEN accessed without authorization a USW computer located in the Western District of Pennsylvania with hostname L*************8.

kk. On or about March 7, 2012, Defendant WEN transmitted a file named "gu.exe" to a USW computer.

ll. On or about March 7, 2012, Defendant WEN stole hundreds of e-mails from the accounts of six USW employees.

mm. On or about April 12, 2012, Defendant WEN accessed without authorization an ATI computer located in the Western District of Pennsylvania with hostname L*****3.

nn. On or about April 12, 2012, Defendant WEN executed the program named "ugls.exe" to monitor the status of compromised ATI computers located in the Western District of Pennsylvania and elsewhere.

oo. On or about April 13, 2012, Defendant WEN accessed without authorization an ATI computer located in the Western District of Pennsylvania with hostname A******5.

pp. On or about April 13, 2012, Defendant WEN transmitted a file named "ccapp.exe" to an ATI computer located in the Western District of Pennsylvania with hostname A******7.

qq. On or about April 13, 2012, Defendant WEN transmitted a file named "i.exe" to an ATI computer located in the Western District of Pennsylvania with hostname A******0.

rr. On or about April 13, 2012, Defendant WEN stole ATI network usernames and passwords for more than 7,000 ATI employees.

ss. On or about May 3, 2012, Defendant WEN accessed without authorization a SolarWorld computer using malware named "ugls.exe" and stole e-mails and files belonging to three employees.

tt. On or about May 9, 2012, Defendant WEN accessed

without authorization a SolarWorld computer using malware named "ugls.exe" and stole e-mails and files belonging to four employees.

uu. On or about July 27, 2012, Defendant WEN accessed without authorization a SolarWorld computer using malware named "ugls.exe" and stole e-mails and files belonging to five employees.

vv. On or about February 20, 2013, WEN changed the registration information for malicious domain accounts "arrowservice.net," "businessconsults.net," "newsonet.net," and "purpledaily.com," and "marsbrother.com."

ww. In or about April 2014, an unidentified co-conspirator created a malicious domain and configured it to resolve to an IP address in Germany.

All in violation of Title 18, United States Code, Section 1030(b).

COUNTS TWO THROUGH NINE
(Computer Fraud and Abuse)

The Grand Jury further charges:

45. The allegations set forth in paragraphs 1-42 and 44 of this Indictment are incorporated herein as if set forth in full.

46. Beginning at least on or about February 26, 2010 and continuing until at least on or about April 13, 2012, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
  a/k/a "Jack Wang,"
  a/k/a "UglyGorilla,"
SUN KAILIANG,
  a/k/a "Sun Kai Liang,"
  a/k/a "Jack Sun,"
WEN XINYU,
  a/k/a "Wen Xin Yu,"
  a/k/a "WinXYHappy,"
  a/k/a "Win_XY,"
  a/k/a "Lao Wen,"
HUANG ZHENYU,
  a/k/a "Huang Zhen Yu,"
  a/k/a "hzy_lhx," and
GU CHUNHUI,
  a/k/a "Gu Chun Hui,"
  a/k/a "KandyGoo,"

aided and abetted by others known and unknown to the Grand Jury, did intentionally access a computer without authorization and exceed authorized access to a computer, and did thereby obtain and attempt to obtain information from a protected computer, for the purpose of commercial advantage and private financial gain, in furtherance of a criminal and tortious act in violation of the laws of Pennsylvania, namely, Invasion of Privacy, and where

the value of the information obtained exceeded, and if completed, would have exceeded, $5,000.

47. On or about the dates identified in Column B of the chart set forth below, each date constituting a separate count as set forth in Column A, Defendants WANG, SUN, WEN, HUANG, and GU, accessed without authorization, and exceeded authorized access to, at least one protected computer belonging to the victim listed in Column C, which was located in the Western District of Pennsylvania, using a computer located outside of the Commonwealth of Pennsylvania. As a result of such unauthorized access and exceeding authorized access, Defendants WANG, SUN, WEN, HUANG, and GU obtained the information listed in Column D.

A Count	B Date (On or About)	C Victim	D Stolen Information
2	2/26/2010	U.S. Steel	Information about 1,753 U.S. Steel computers.
3	5/6/2010	Westinghouse	Proprietary and confidential files related to the AP1000 nuclear power plant.
4	12/30/2010	Westinghouse	Information from e-mail accounts of Westinghouse employees A.C., D.C., X.L, R.P, W.P, and C.P.
5	1/3/2011	Westinghouse	Information from e-mail accounts of Westinghouse employees A.C., D.C., X.L, R.P, W.P, and C.P.
6	1/5/2011	Westinghouse	Information from e-mail accounts of Westinghouse employees A.C., D.C., X.L., M.F., R.K., and F.S.

A Count	B Date (On or About)	C Victim	D Stolen Information
7	1/31/2012	USW	Information from e-mail accounts of USW employees L.G., C.L., H.H., W.D., J.G., and G.P.
8	3/7/2012	USW	Information from e-mail accounts of USW employees L.G., C.L., H.H., W.D., G.H., L.A., L.B., and C.K.
9	4/13/2012	ATI	ATI network credentials for thousands of ATI employees.

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030 (c)(2)(B)(i)-(iii), and 2.

COUNTS TEN THROUGH TWENTY-THREE
(Damaging a Computer)

The Grand Jury further charges:

48. The allegations set forth in paragraphs 1-42 and 44 of this Indictment are incorporated herein as if set forth in full.

49. Beginning at least on or about February 8, 2010 and continuing until at least on or about April 13, 2012, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
a/k/a "Jack Wang,"
a/k/a "UglyGorilla,"
SUN KAILIANG,
a/k/a "Sun Kai Liang,"
a/k/a "Jack Sun,"
WEN XINYU,
a/k/a "Wen Xin Yu,"
a/k/a "WinXYHappy,"
a/k/a "Win_XY,"
a/k/a "Lao Wen,"
HUANG ZHENYU,
a/k/a "Huang Zhen Yu,"
a/k/a "hzy_lhx," and
GU CHUNHUI,
a/k/a "Gu Chun Hui,"
a/k/a "KandyGoo,"

aided and abetted by others known and unknown to the Grand Jury, did knowingly cause and attempt to cause the transmission of a program, information, code, and command, and, as a result of such conduct, did intentionally cause damage and attempt to cause damage without authorization to a protected computer, and which offense caused, and would, if completed, have caused, loss aggregating at least $5,000 in value to at least one person

during a one-year period from a related course of conduct, and damage affecting at least ten protected computers during a one-year period.

50. On or about the dates identified in Column B of the chart set forth below, each date constituting a separate count as set forth in Column A, Defendants WANG, SUN, WEN, HUANG, and GU did knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, did intentionally cause damage and attempt to cause damage without authorization to a protected computer belonging to the victim listed in Column C. Each offense caused and would, if completed, have caused loss aggregating at least $5,000 in value to at least one person during a one-year period from a related course of conduct, and damage affecting at least ten protected computers during a one-year period. A summary of the method of transmission of the malicious program, information, code, and command is listed in Column D.

A Count	B Date (On or About)	C Victim	D Description of Transmission
10	2/8/2010	U.S. Steel	Spearphishing e-mail to U.S. Steel employee R.G. with subject "Meeting Invitation," which contained the malicious file "agenda.zip."
11	5/6/2010	Westinghouse	Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname

A Count	B Date (On or About)	C Victim	D Description of Transmission
			L******0.
12	5/6/2010	Westinghouse	Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname W*****9.
13	12/30/2010	Westinghouse	Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname L******9.
14	12/30/2010	Westinghouse	Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname T********4.
15	1/3/2011	Westinghouse	Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname W*****9.
16	1/3/2011	Westinghouse	Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname T********9.
17	1/5/2011	Westinghouse	Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname L******4.
18	1/5/2011	Westinghouse	Transfer of at least one malicious program, information, code, and command to a Westinghouse computer with hostname to L******5.
19	1/31/2012	USW	Transfer of at least one malicious program, information, code, and command to a USW computer with hostname

A Count	B Date (On or About)	C Victim	D Description of Transmission
			J*************6.
20	3/7/2012	USW	Transfer of at least one malicious program, information, code, and command to a USW computer.
21	4/13/2012	ATI	Transfer of at least one malicious program, information, code, and command to an ATI computer with hostname A******7.
22	4/13/2012	ATI	Transfer of at least one malicious program, information, code, and command to an ATI computer with hostname A******0.
23	4/13/2012	ATI	Transfer of at least one malicious program, information, code, and command to an ATI computer with hostname K******I.

All in violation of Title 18, United States Code, Section 1030(a)(5)(A) and 1030(c)(4)(B), and 2.

COUNTS TWENTY-FOUR THROUGH TWENTY-NINE
(Aggravated Identity Theft)

The Grand Jury further charges:

51. The allegations set forth in paragraphs 1-42 and 44 of this Indictment are incorporated herein as if set forth in full.

52. Beginning at least on or about December 30, 2010 and continuing until at least on or about April 12, 2012, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
a/k/a "Jack Wang,"
a/k/a "UglyGorilla,"
SUN KAILIANG,
a/k/a "Sun Kai Liang,"
a/k/a "Jack Sun,"
WEN XINYU,
a/k/a "Wen Xin Yu,"
a/k/a "WinXYHappy,"
a/k/a "Win_XY,"
a/k/a "Lao_Wen,"
HUANG ZHENYU,
a/k/a "Huang Zhen Yu,"
a/k/a "hzy_lhx," and
GU CHUNHUI,
a/k/a "Gu Chun Hui,"
a/k/a "KandyGoo,"

aided and abetted by others known and unknown to the Grand Jury, during and in relation to the crime of conspiracy to commit computer fraud in violation of Title 18, United States Code, Section 1030(b), as more fully set forth in Count One above, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person.

53. On or about the dates identified in Column B of the chart set forth below, each date constituting a separate count as set forth in Column A, Defendants did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, listed by initials in Column C, who was associated with a victim listed in Column D.

A Count	B Date (On or About)	C Means of Identification Belonging to	D Victim
24	12/30/2010	D.C.	Westinghouse
25	1/3/2011	D.C.	Westinghouse
26	1/5/2011	D.C.	Westinghouse
27	1/31/2012	L.G.	USW
28	3/7/2012	L.G.	USW
29	4/13/2012	P.V.	ATI

All in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), and 2.

COUNT THIRTY
(Economic Espionage)

The Grand Jury further charges:

54. The allegations set forth in paragraphs 1-42 and 44 of this Indictment are incorporated herein as if set forth in full.

55. On or about May 6, 2010, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
a/k/a "Jack Wang,"
a/k/a "UglyGorilla,"
SUN KAILIANG,
a/k/a "Sun Kai Liang,"
a/k/a "Jack Sun,"
WEN XINYU,
a/k/a "Wen Xin Yu,"
a/k/a "WinXYHappy,"
a/k/a "Win_XY,"
a/k/a "Lao Wen,"
HUANG ZHENYU,
a/k/a "Huang Zhen Yu,"
a/k/a "hzy_lhx," and
GU CHUNHUI,
a/k/a "Gu Chun Hui,"
a/k/a "KandyGoo,"

aided and abetted by others unknown to the Grand Jury, intending and knowing that the offense would benefit a foreign government, instrumentality, and agent, namely China, did knowingly and without authorization copy, download, upload, replicate, transmit, deliver, send, mail, communicate, and convey a trade secret, and did attempt to do so, specifically a file named "wd.rar" containing proprietary and confidential technical and design specifications, owned by Westinghouse, which were related

to the pipes, pipe supports, and pipe routing within the AP1000 nuclear power plant.

All in violation of Title 18, United States Code, Sections 1831(a)(2) & (a)(4), and 2.

COUNT THIRTY-ONE
(Theft of a Trade Secret)

The Grand Jury further charges:

56. The allegations set forth in paragraphs 1-42 and 44 of this Indictment are incorporated herein as if set forth in full.

57. On or about May 6, 2010, in the Western District of Pennsylvania and elsewhere, Defendants

WANG DONG,
a/k/a "Jack Wang,"
a/k/a "UglyGorilla,"
SUN KAILIANG,
a/k/a "Sun Kai Liang,"
a/k/a "Jack Sun,"
WEN XINYU,
a/k/a "Wen Xin Yu,"
a/k/a "WinXYHappy,"
a/k/a "Win_XY,"
a/k/a "Lao_Wen,"
HUANG ZHENYU,
a/k/a "Huang Zhen Yu,"
a/k/a "hzy_lhx," and
GU CHUNHUI,
a/k/a "Gu Chun Hui,"
a/k/a "KandyGoo,"

aided and abetted by others unknown to the Grand Jury, with the intent to convert a trade secret to the economic benefit of someone other than Westinghouse, and intending and knowing that the offense would injure Westinghouse, did knowingly and without authorization copy, duplicate, download, upload, replicate, transmit, deliver, send, mail, communicate, and convey a trade secret, and attempt to do so, specifically, a file named "wd.rar" containing proprietary and confidential technical and

design specifications, owned by Westinghouse, which were related to the pipes, pipe supports, and pipe routing in a product, namely the AP1000 nuclear power plant, that was produced for and placed in interstate and foreign commerce.

All in violation of Title 18, United States Code, Sections 1832(a)(2) & (a)(4) and 2.

A true bill,

[redacted]

FOREPERSON

DAVID J. HICKTON
United States Attorney
PA ID No. 34524

EXHIBIT A

Wang Dong

a/k/a "Jack Wang,"

a/k/a "UglyGorilla"



EXHIBIT B

SUN KAILIANG,

a/k/a “Sun Kai Liang,”

a/k/a “Jack Sun”



军人礼赞 PHOTO BY HEX

<u>**EXHIBIT C**</u>

WEN XINYU,

a/k/a “Wen Xin Yu,”

a/k/a “WinXYHappy,”

a/k/a “Win_XY,”

a/k/a “Lao Wen”



EXHIBIT D

HUANG ZHENYU,

a/k/a “Huang Zhen Yu,”

a/k/a “hzy_lhx”



EXHIBIT E

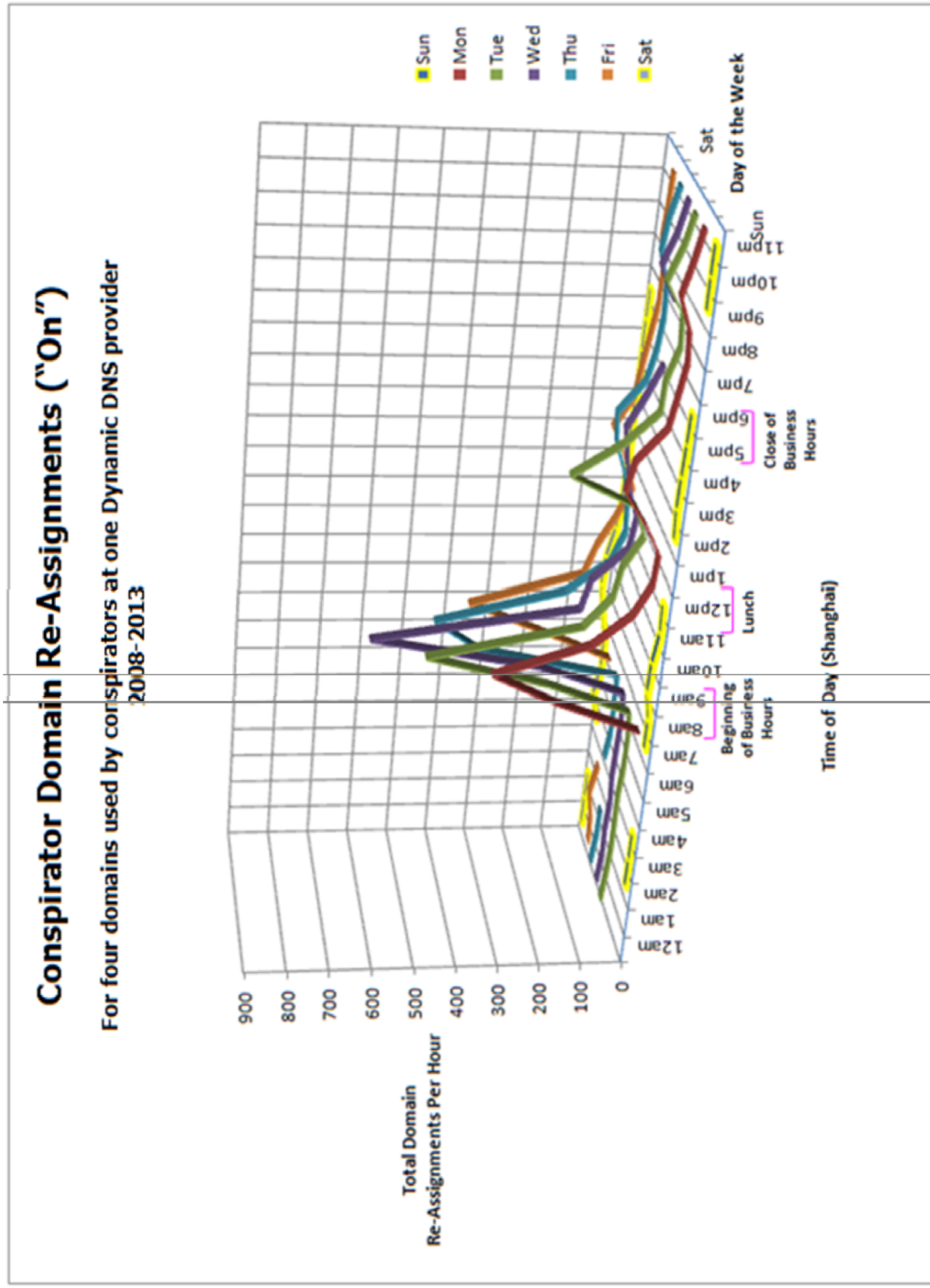
GU CHUNHUI,

a/k/a “Gu Chun Hui,”

a/k/a “KandyGoo”

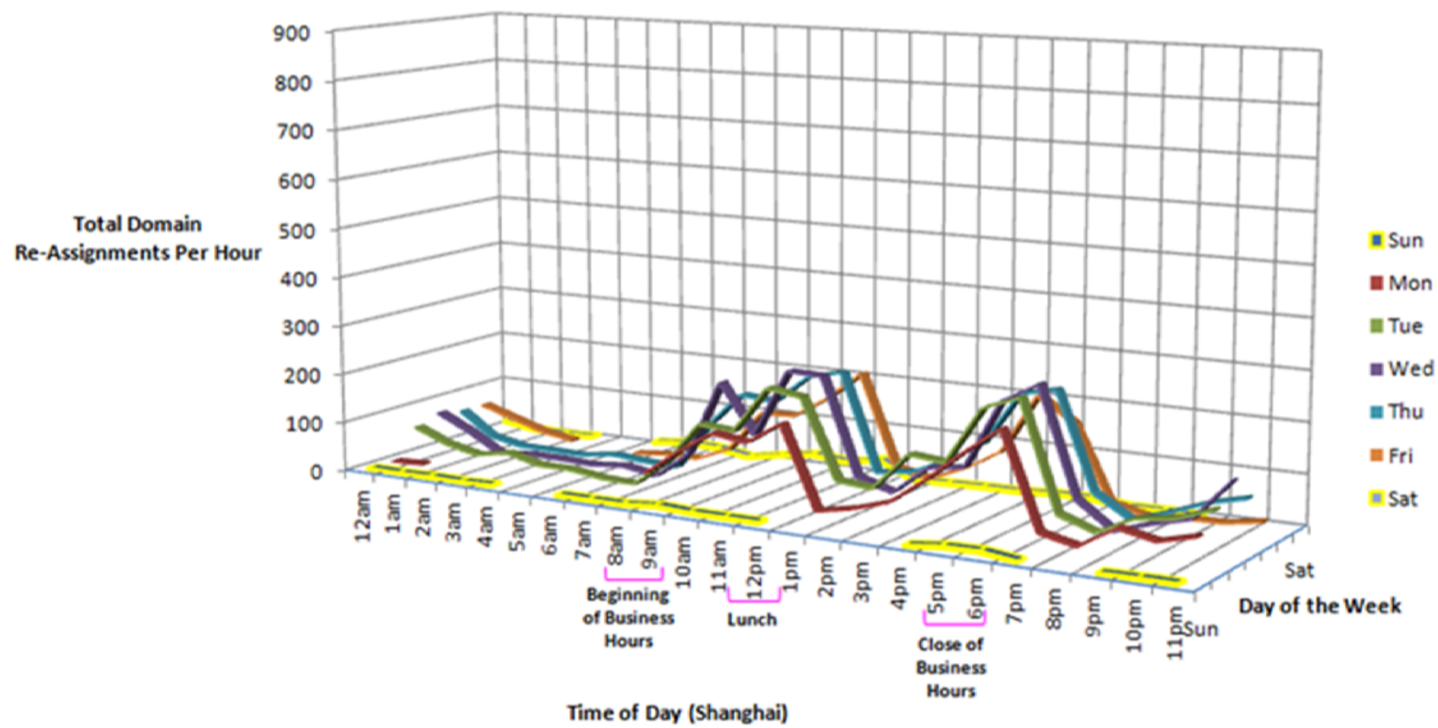


EXHIBIT F


Conspirator Domain Re-Assignments ("On")
For four domains used by conspirators at one Dynamic DNS provider
2008-2013
Total Domain
Re-Assignments Per Hour
900
800
700
600
500
400
300
200
100
0
12am
1am
2am
3am
4am
5am
6am
7am
8am
9am
10am
11am
12pm
1pm
2pm
3pm
4pm
5pm
6pm
7pm
8pm
9pm
10pm
11pm
Beginning of Business Hours
Lunch
Close of Business Hours
Time of Day (Shanghai)
Sun
Sat
Day of the Week
Sun
Mon
Tue
Wed
Thu
Fri
Sat

Conspirator Domain Re-Assignments ("Off")

For four domains used by conspirators at one Dynamic DNS provider 2008-2013



Conspirator Domain Re-Assignments ("On" and "Off")

For four domains used by conspirators at one Dynamic DNS provider 2008-2013

